1999/23 Lifestyle

https://shop.jungle.world/artikel/1999/23/liegt-unterm-abstreifer

Liegt unterm Abstreifer

Von **fabian sänger**

Die Bundesregierung lehnt die Beschränkung der Datenkryptographie ab, gibt aber ein schlechtes Vorbild

Bevor es ins Detail geht, die gute Nachricht: Wer verbotene Zeitungen herausgeben, Banküberfälle verabreden oder Listen mit Anschlagszielen zu Hause aufbewahren möchte, kann dies auch künftig per Computer tun. Natürlich verschlüsselt, am besten mit PGP (Pretty Goud Privacy), dem Lieblingsverschlüsselungsprogramm der Linken (auch der Rechten übrigens). Auch die stärksten CIA-Computer scheitern an solchen Kryptographien.

Das ist auch der Grund, weshalb der frühere Innenminister Manfred Kanther beabsichtigte, das freie Verschlüsseln von Daten einzuschränken. Ein Kommunikationsraum, der sich dem Einblick der Herrschenden entzieht - das ist Bedrohungsszenario für die Kontrolleure.

Daß sich jetzt im Kabinett der Bundesregierung doch noch die Meinung durchsetzte, von Reglementierungen der Kryptographie abzusehen, ist einer merkwürdigen Koalition von KryptobefürworterInnen zu verdanken. Die reicht vom ehemaligen Wirtschaftsminister Günther Rexrodt (FDP) über Computer Bild, Gruner & Jahr, Stiftung Warentest, IG Medien, dem Bundesverband Deutscher Banken, der Gesellschaft für Datenschutz und Datensicherheit bis zum Chaos Computer Club.

An dem Zustandekommen eines solch breiten Bündnisses hatte vor allem der Referatsleiter für Informationssicherheit im Wirtschaftministerium, Ulrich Sandl, gebastelt, der kürzlich unter bisher ungeklärten Umständen aus dem Fenster stürzte und sich schwer verletzte. In der Netzgemeinde kursieren seitdem diverse Verschwörungstheorien. Schließlich ist bekannt, daß es auch eine starke Gegenbewegung gibt, vor allem in Geheimdienst- und Sicherheitskreisen, die eine Behinderung der Strafverfolgung befürchten.

Auch das Innenministerium unter Otto Schily schien lange Zeit nicht so richtig von der Freigabe kryptographischer Verfahren überzeugt. Daß Schily am vergangenen Dienstag dennoch seine Unterschrift unter die von Ulrich Sandl erarbeitete Kabinettsvorlage "Eckpunkte der deutschen Kryptopolitik" setzte, dürfte einer Kompromiß-Klausel in dem Papier zu verdanken sein, die besagt, daß das Geschehen im Netz nach Sicherheitskriterien zwei Jahre lang beobachtet wird, um dann die Entscheidung gegebenenfalls zu revidieren. Zur Zeit gebe es zwar kein relevantes Sicherheitsproblem durch die freie Verfügbarkeit von Verschlüsselungssoftware, aber es könne schließlich keiner wissen, wie sich das entwickelt.

In dem Papier heißt es, Verschlüsselungstechniken dürften in Deutschland auch künftig "ohne Restriktion entwickelt, hergestellt, vermarktet und genutzt werden". Nur die weite Verbreitung sicherer Verschlüsselungssysteme ermögliche einen wirksamen Schutz von Unternehmensgeheimnissen und anderen sensiblen Daten. Sie sei damit eine entscheidende Voraussetzung für die Fortentwicklung des elektronischen Geschäftsverkehrs. "Ein weiteres Ziel der Bundesregierung" sei, heißt es weiter, die "Stärkung der Leistungsfähigkeit und der internationalen Wettbewerbsfähigkeit der deutschen Kryptohersteller."

Es sind also in erster Linie ökonomische Interessen, die die Regierung diesen Kurs hat einschlagen lassen. Kaufen und Verkaufen per Internet, elektronische Börsen- und Bankgeschäfte - das alles geht nur bei völliger Vertraulichkeit der Daten. Auch zum Schutz vor Wirtschaftsspionage ist die Verschlüsselung der Daten unerläßlich. Das haben Hacker oft genug demonstriert.

Es kommt sicher nicht allzu häufig vor, daß Interessen der Wirtschaft mit demokratischen Interessen so gut zusammenpassen. Ein liberales Crossover sozusagen. Zur Kryptolobby gehört allerdings bei Wirtschaft wie bei Linken jeweils nur ein kleiner Kreis von ExpertInnen. In der linken Szene verwenden bisher nur wenige wirklich ein Verschlüsselungsprogramm. Zu unkomfortabel ist etwa PGP, das einfach nicht auf der Windows-Oberfläche laufen will. Auch in der Wirtschaft verschlüsseln nach einer Umfrage vom September 1998 nur vier Prozent der deutschen Unternehmen ihre elektronische Post. Die Bundesregierung hat daher nun beschlossen, die Sensibilisierung der NutzerInnen in diesem Bereich zu fördern.

Ein Schritt, der auch von der medienpolitischen Sprecherin der PDS-Bundestagsfraktion, Angela Marquardt, begrüßt wird. Trotzdem kritisierte sie das Eckpunktepapier der Regierung: "Es findet sich darin kein Wort zu Key Recovery", erklärte sie gegenüber Jungle World: "Vermutlich will sich die Regierung diese Option offenhalten." Bei Key Recovery handelt es sich um ein Verfahren, bei dem bei staatlichen Behörden ein "Nachschlüssel" für die verschlüsselten Daten hinterlegt wird, so daß diese einen Zugriff auf die codierten Texte haben. Ex-Bundesinnenminister Kanther hatte vorgeschlagen, die Implementierung von Key Recovery zur Bedingung für die Verfügbarkeit von Kryptosoftware zu machen. Vorbild waren die USA. Nach den inzwischen geänderten Ausfuhrbestimmungen durften nur Kryptoprodukte mit einem relativ schwachen Schlüssel von 40 Bits exportiert werden. Bei stärkeren Schlüsseln hatte für die darüber hinausgehenden Bits ein Nachschlüssel bei der US-Regierung, konkret der National Security Agency, zu verbleiben.

In vorauseilendem Gehorsam schlossen sich in den USA 30 Softwareproduzenten zu einer Key Recovery Alliance zusammen, darunter IBM, Hewlett-Packard, Toshiba und auch die PGP-Mutterfirma Network Associates. Seitdem produziert Network Associates neue, kommerzielle PGP-Versionen nur noch mit implementiertem Key Recovery. Als sicher gelten daher nur noch die alten, als Freeware kostenlos im Internet verfügbaren PGP-Versionen, die allerdings sehr unkomfortabel in der Handhabung sind.

Als "Referenzprodukt" für Key Recovery gilt laut CCC ein Kryptoprogramm von IBM mit dem Namen Lotus Notes. Dieses wird zur Zeit bei der Verwaltung der Bundeswehr eingeführt. Von den 64 Bits Schlüssellänge, verbleiben laut Produktbeschreibung 24 Bits bei der US-Regierung, weshalb der CCC der Bundeswehr vom Einsatz dieses Produktes ohne weitere Maßnahmen dringend abgeraten hat. Ob es allerdings wirklich diese Version von Lotus Notes ist, die gerade bei der Bundeswehr eingeführt wird, ist nicht bekannt. Eine Kleine Anfrage von Marquardt von

Anfang Mai wurde bis heute nicht beantwortet.

Im Bundeswirtschaftsministerium widersprach man sich anfangs ein paar Mal und erklärte dann, es handele sich um eine neue Version ohne Key Recovery-Funktion. Sie habe eine Schlüssellänge von 56 Bits, doch auch "das ist alles andere als eine starke Verschlüsselung", kritisiert Marquardt. Dem widerspricht auch das Wirtschaftsministerium nicht: Die aktuelle Lotus-Version sei wegen der geringen Schlüssellänge "nicht für Bereiche höherer Sicherheit geeignet", erklärt Referatsleiter Sandl.

"Es ist nicht so, daß ich mir Tag und Nacht Gedanken um die Sicherheit der Bundeswehrkommunikation mache", erläutert Marquardt ihre Kritik an dem Erwerb von Lotus Notes. "Aber dieses kryptische Verhältnis zwischen Worten und Taten der Bundesregierung läßt mich an der Aussagekraft der Kabinettserklärung zweifeln." Nicht nur, daß man ein Produkt einer Firma kaufe, die sich als Mitglied der Key Recovery Alliance für das Hinterlegen von Nachschlüsseln stark macht. Nicht nur, daß man auf ein veraltetes Kryptoprodukt mit viel zu schwachem Schlüssel setze, es sei auch ein Widerspruch zu dem Vorhaben, die deutschen Kryptohersteller zu fördern, wenn man sich ausgerechnet ein IBM-Produkt zulege.

In der Tat scheint bei der Bundesregierung die eine Hand nicht immer zu wissen, mit was die andere gerade verschlüsselt. Mit dieser Überforderung ist man aber wahrlich nicht allein in der Gesellschaft. Aufklärung und die Entwicklung leicht klick-barer Kryptoanwendungen sind die Voraussetzung für einen massenhaften Einsatz von Verschlüsselungsprogrammen. Wenn schon die Bundesregierung nicht mit gutem Vorbild vorangeht, sollte das die linke Szene tun und per Kryptographie den Lauschangreifern einen Strich durch die Rechnung machen.